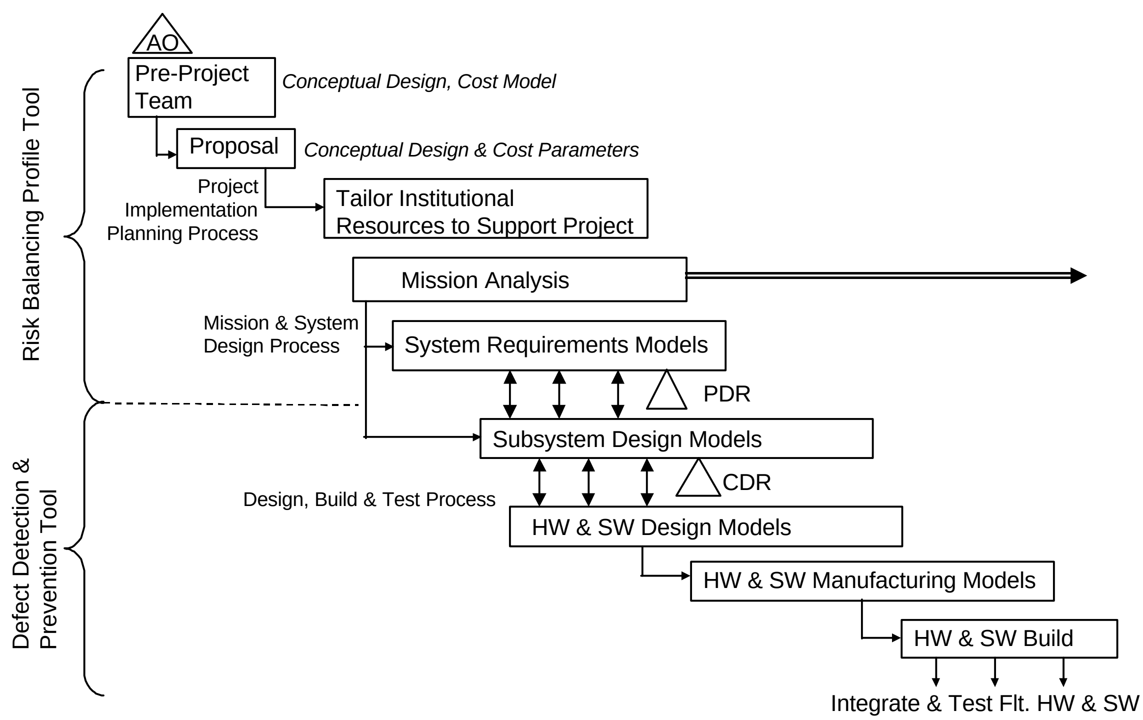
Risk Balancing Profile Tool

Dr. Michael A. Greenfield, Deputy Associate Administrator for Safety and Mission Assurance
National Aeronautics and Space Administration
Washington, D.C. 20546

Introduction

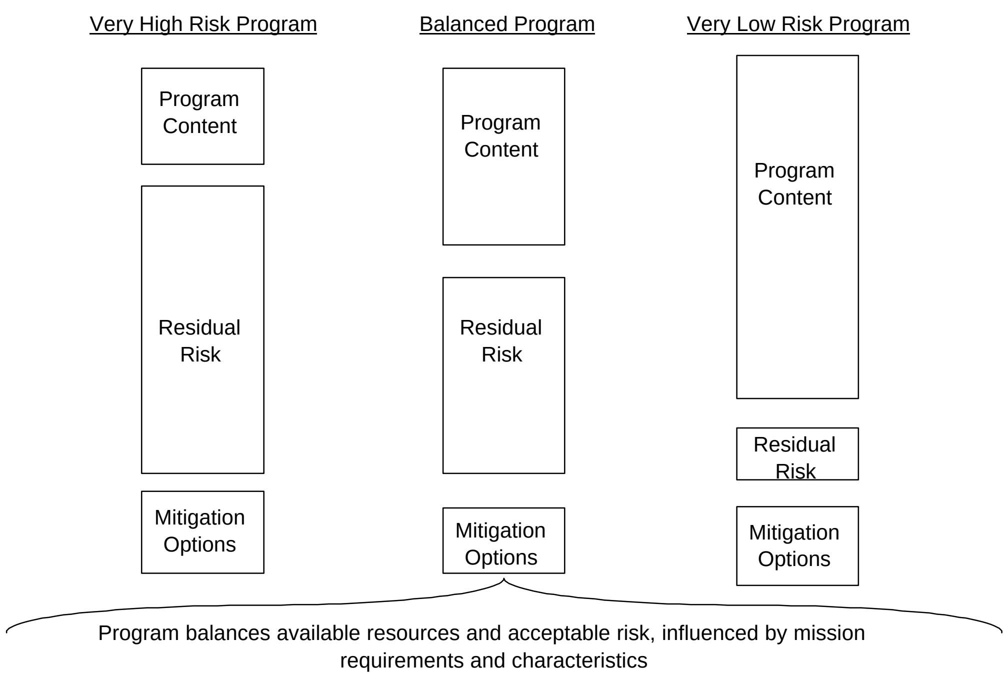
Although a "rule-based" fixed requirements-driven approach in the past served the Agency well in the safety and mission assurance disciplines, those days are now over. The time when every identifiable step was taken to avoid risk is being replaced by a "faster, better, cheaper" approach which requires that risk be managed differently. NASA is moving to a "knowledge-based" approach. Key to this approach will be the newly developed Risk Balancing Profile (RBP) Guide. This guide is part of the Office of Safety and Mission Assurance's new thrust to reduce the risk in NASA flight programs by providing tools and techniques to enable projects to develop and implement an effective, tailored mission assurance program. This activity is an outgrowth of the concept presented in a previous paper, IAA-97-IAA.6.2.06, "Risk as a Resource." In that paper, the concept of trading and accepting subsystem risks to arrive at an optimal overall spacecraft risk posture was presented. The RBP Guide is a compendium of risk data that will provide a mechanism early in project formulation (see below) for identifying residual performance risk associated with risk-reducing program content. It identifies mitigation possibilities corresponding to residual performance risk and relate appropriate resource considerations for the program content. This tool provides direction on the sorting out of possibilities and consequences for spending resources against program or performance risk.



This paper details the trades that can be made early to achieve an optimal risk posture. Another tool, Defect Detection and Prevention, addressing the optimization of preventative actions chosen during project implementation (design, build and test) is the subject of another paper.

The Risk Balancing Profile approach recognizes that risk mitigation options within a program or project must be balanced against available cost and schedule constraints while providing the appropriate level of mission success. The graphic below provides a notional picture of the process. The right hand column approach for a very low risk (VLR) program does everything possible to eliminate risk. The content for program risk mitigation is large; the residual risk is low. Some further mitigation options are also possible if needed. The left hand column program content represents a program approach which by doing less accepts a very much higher risk (VHS) to success. The residual risks are high although some mitigation is possible. Unfortunately, the very low risk approach is generally too expensive except for the most demanding missions such as human space flight. Somewhere in between the two extremes lies the optimal risk management program. The Safety and Mission Assurance professional must work with the project manager early in the project's formulation phase to craft the "balanced" approach. Development of a balanced program would entail thoughtful choice of what risk mitigation actions provide the greatest cost benefit based on the marginal cost of each risk reducing action.

Overview of Risk Balancing Profile Approach



Such an approach to a Electronics Parts Program is presented below. As in all cases, the project manager must make informed decisions on where to spend his or her risk reduction dollars. Key content areas are part screening, technology conformance inspection, radiation hardness, and management approaches. Under each area are listed the standard engineering risk mitigating activities with an alphanumeric designator. The VLR program content lists all such options. Residual risks are numbered.

Many "better, faster, cheaper" projects are faced with the challenge of developing an optimal parts program. The RBP tool provides a qualitative risk balancing guide to support the complex decision process. For an example, consider the screening section of content for a VLR program. A project utilizing “S1”, ESD sensitivity testing (per Mil-std 833), would mitigate the risk of ESD vulnerability (residual risk 1) that may be present in a VHR approach. However, a project manager may choose to perform only ESD awareness training (see Mitigations) and accept slightly higher risk in this area.

Risk Balancing Profile-Electronic Parts Program

Very High Risk Electronic Parts Program	Tailored Approach	Very Low Risk Electronic Parts Program
Program Content	**Prog.Content**	**Program Content (For Class V Compliant Part)**
<u>Testing(freq. & conditions vary with mfr internal procedures)</u> S8 – burn-in, time and temperature will vary(may not be done at all) S10 –electrical test (usually room temperature only) S12 – external visual **<u>Technology Conformance Inspection(TCI)</u>** None **<u>Radiation Hardness Asurance(RHA)</u>** None **<u>Related Management</u>** None	***As Selected (Tailored to be Project Specific)***	**<u>Screening*(done on every part)</u>** S1 – ESD sensitivity. Test method (tm) 3015, 4.2.3[@] S2 – nondestructive bond pull (NDBP), tm 2023 S3 – internal visual. tm 2010, condition A S4 – temperature cycling. tm 1010, condition C, min. 50 cycles S5 – constant acceleration. tm 2001, condition E S6 – Particle Impact Noise Detection (PIND), tm 2020 S7 – radiograph inspection, tm 2012 S8 – burn-in (forward and reverse bias). tm 1015, 160-240hr @ 125C minimum; pre and post burn-in interim electrical parameter test according to device specification . S9 – PDA calculation, 5% of all lots. S10 – final electrical test: static, dynamic / functional, and switching test at three temperatures. Table III of mil-prf-38535E. S11 – seal, tm 1014 S12 – external visual, tm 2009 * For details on all of the above, refer to App. B of mil-prf-38535E. Refer to JPL document D-16389 for Known Good Die standards. [@]test methods can be found in Mil-std-883. **<u>Technology Conformance Inspection (TCI)[#]</u>** T1 – Group A electrical test, performed on each lot unless already done for S7. T2 – Group B tests: resistance to solvents(tm 2015), bond strength(tm 2011), die shear(tm 2019), stud pull(tm 2027), solderability (tm 2003). Must be done on real devices, can be rejects from previous testing. T3 – Group C tests: steady-state life test (tm 1005) and end-pt electrical parameters. Performed on each wafer lot. T4 – Group D tests: physical dimensions, lead integrity, seal, thermal shock, moisture resistance, shock, vibration, salt atmosphere, internal water vapor, lid torque, etc. Performed on initial production lot of the package family. [#]For minimum sample size, see Tables II, III, IV, and V of mil-prf-38535E. Additional requirements are in App. B.4. **<u>Radiation Hardness Asurance(RHA)</u>** R1 – Total Ionizing Dose. Tm 1019 R2 – Single event effects. ASTM F-1192 or EIA/JESD 57 R3 – Neutron Irradiation. Tm 1017 R3 only done when project deem necessary. **<u>Related Management</u>** M1 – QML program per mil-prf-38535E, app. G. M2 – Traceability Mil-std-38535E, 3.1
Residual Risks	**Residual Risks**	**Residual Risks**
1. Vulnerability to ESD – S1 2. Vulnerability to temperature extremes – S4, T4 3. Vulnerability to radiation environments – R1, R2 4. Vulnerability to physically harsh environments – T2, T4 5. Poor workmanship – S2, S3, S5, S6, S7, S11, S12, T2 6. No traceability – M2 7. Latent defects could cause the system to fail or not meet its requirements – S8 8. Choosing unreliable contractor to produce parts – M1 9. Use of parts from lots with marginal reliability – S9 10. Unknown time-dependent electrical behavior – T3 11. Unknown radiation risk – R1, R2 12. Unknown functional and system margins – S4, T1, R1, R2 13. Unknown reliability for plastic parts – general 14. Non-homogeneous parts – general. 15. Parts tested may not be representative of the lot – general 16. Date codes gives no useful information – general 17. Failing parts during testing phase may cause project delay and overbudget – general 18. Unknown failure mechanisms – general 19. Encountering natural environments(radiation, physical mechanisms) not accounted and/or tested for – general	***Residual Risk For Program Content Selected***	18. Unknown failure mechanisms – general Encountering natural environments (radiation, temperature, physical mechanisms) not accounted and/or tested for – general
Mitigations (Risk reduction)	**Mitigations**	**Mitigations (Risk Reduction)**
- Reusing high quality proven parts (3,5,7,8,9,10,11,12,13,18) - ESD awareness/training(1) - Parts List Evaluation/involve parts specialist(all except 14,15,16,17,19) - Procure Grade 1 parts(5,9,13,14,15,16) - Parts Construction Analysis(5) - Destructive Physical Analysis(5) - Burn-in/Life testing(7,10) - Radiation Testing(3,11) - Incentivize contractor(8) - Simulation of the flight environment(11,12,18) - Identify critical functions(general)	***Mitigations of Residual Risk***	- Perform wide temperature testing (18) - Review GIDEP Alerts/Lessons learned(general) - Incentivize contractor(general) - Cross training(general)

A similar approach can be used for project management approaches such as Risk Management Planning. As can be seen below in the Risk Management Plan development example of an RBP, the two extremes of possible approaches are presented. The right hand column would represent an approach that would result in very low program risk; almost everything that can be done is done. The program content includes extensive risk planning activities (RP1-RP5), a robust risk identification and assessment process (RA1-RA8), a full risk decision-making approach (RD1-RD7),

Risk Balance Profile - Risk Management Program

Very High Risk Risk Management Program	**Tailored Approach**	**Very Low Risk Risk Management Program**
Program Content	**Prog.Content**	**Program Content**
Risk Planning **RP1** - A risk management process implemented throughout the project/task life cycle. **RP5**$_{\chi}$ - Develop a RM strategy consistent with project constraints. **RP7 –** Write an RM plan in accordance with the NASA RM policy for approval by the Program Manager (PM). **Risk Identification and Assessment** **RA1** - Identify general risk issues and concerns. **RA4**$_{\chi}$ - Identify risks to the subsystem level. **RA5** – Conduct qualitative risk assessments for each risk item, and for the total project risk. **RA7**$_{\chi}$ - Assess the overall risk (combined implementation risk and mission risk) for each risk item. **Risk Decision-Making** **RD1**$_{\chi}$ – Document high priority risks as defined by the PM. **RD4** – Take risk mitigation actions as decided by the PM. **RD5**$_{\chi}$ – Record risk decisions through project management reporting mechanisms as defined in the RM plan. **Risk Tracking and Reporting** **RT2**$_{\chi}$ – Track the project and its aggregate risk position. **RT3** – Manage & track technical margin. **RT5**$_{\chi}$ - Prepare risk status reports (quarterly).	**As Selected (Tailored to be Project Specific)**	**Risk Planning** **RP1** - A risk management process implemented throughout the project/task life cycle. **RP2** - Obtain initial data (project context/constraints) as required to develop a comprehensive risk management strategy/methodology. **RP3** - Identify major areas of project risk and related mitigation plans. **RP4** - Make contingency plans based on available descope options. **RP5** - Define overall project RM methodology (flow chart). **RP6** - Identify project-unique risk identification/ranking methods. **RP7 - –** Write an RM plan in accordance with the JPL RM policy for approval by the PM. **Risk Identification and Assessment** **RA1** - Identify general risk issues and concerns (Project team/experts/LL). **RA2** – Systematically identify specific risks (checklists, Risk Identification & Mitigation Database queries, or comprehensive processes). **RA3** – Identify threats to project reserves. **RA4** – Employ project team to identify risks to the major assembly level. **RA5** - Perform qualitative risk assessment for prelim. screening of risks. **RA6** - Perform quantitative risk assessment , determine the probability estimate for each event, and aggregate risks . **RA7** - Assess the implementation risk and mission risk aspects of each risk item. **RA8** - Verify/validate mitigation actions. **Risk Decision-Making** **RD1** - Perform quantitative risk trade-off studies using Significant Risk List (SRL) data to identify proposed mitigation actions. **RD2** – Ensure that proposed mitigation actions include optimization of project reserves (technical and programmatic). **RD3** – Employ project team to review and critique proposals. **RD**4 - Take risk mitigation actions as decided by PM. **RD5** - Record risk acceptance/mitigation decisions in an updated SRL. **RD6** - Publish contingency plans (descope options, Alternative Technology Development Plans, etc.). **RD7** - Publish requirements for risk tracking metrics. **Risk Tracking and Reporting** **RT1 -** Baseline the SRL, descope database. **RT2** - Track SRLs, milestones, and aggregate project risk. **RT3** – Manage & track technical margin (Margin Management Matrix). **RT4** - Track cost, schedule, and reserves. **RT5** - Prepare risk status reports (monthly). **RT6 -** Update the SRL as required by the evolving project. **RT7 -** Perform risk disposition.
Resiual Program Risks	**Residual Program Risks**	**Residual Program Risks**
1. Unknowable residual risk, or inadequate assessment, threatens the achievement of launch and operational capability and mission success (expected science return, demonstration of new technologies, etc.) within cost & schedule constraints – RP6, RA1→RA6 2. Mitigation actions, contingencies, and margins prove inadequate despite the quantitative assessments – RP4, RA8, RD5, RT3 3. The threat to project resources due to unquantified risk to project reserves (technical, cost, and schedule) – RP3, RA6, RA7, RT3, RT4 4. Increased risk due to lack of risk assessment below the subsystem level – RA4	**Residual Program Risk For Program Content Selected**	1. Unknowable residual risk threatens the achievement of launch and operational capability and mission success (expected science return, demonstration of new technologies, etc.) within cost & schedule constraints 2. Mitigation actions, contingencies, and margins prove inadequate despite the quantitative assessments – RA3, RA7, RD2, RD4, RT3

Mitigations (Risk Reduction)	Mitigations	Mitigations (Risk Reduction)
- Increase unallocated margin in project reserves (technical, cost, and schedule), including descope if needed. - 1, 2, 3, 4 - Develop quantitative risk assessments for the High/High or primary risks and regularly assess the impact on reserves. – 1, 3 - Increase mission assurance activities, including maximum use of inherited designs. – 1, 3, 4	**Mitigation of Residual Program Risk Relating to Program Content Selected**	- Maintain adequate unallocated margin in project reserves (technical, cost, and schedule). – 1, 2

χ indicates that the High Risk Program Content item differs in level-of-effort from the corresponding Low Risk item.

and a broad risk tracking and reporting system (RT1-RT7). The project manager must strike the proper balance against available funds and schedule and the amount of acceptable overall risk. Once again the challenge is to determine "how much is enough." Even with such an overall approach, there still are some residual program risks generally in the area of "unknowables." Further risk mitigation may be achieved by maintaining greater unallocated reserves. The left hand VHR approach does considerably less. Another area for risk balancing is the selection of the appropriate design requirements in the early formulation phase. Such an example, Environmental Requirements, is depicted below.

Risk Balance Profile-Environmental Requirements

Very High Risk Environmental Requirements Program	Tailored Approach	Very Low Risk Environmental Requirements Program
Program Content	**Prog.Content**	**Program Content**
<u>Testing</u> See Testing Risk Balance Profile **<u>Environmental Design Requirements</u>** (See M5,E2,E4) D1-Thermal D2- Structural Loads D3-Vibration D4-Acoustic D5- Particle Radiation (Natural & on board sources, Single Event Effects) D6-Electromagnetic and Magnetic Interference D7-Electrostatic Discharge D8- Spacecraft Charging D9-Solid Particles (inc. micrometeoroids, space debris, comet dust, planetary rings) D10-Pyroshock D11-Contamination (inc. purge rqts) D12-Lightning D13-Venting and Repressurization (inc.Launch Pressure Decay, descent) D14-Surface Pressure and Atmosphere D15-Surface Impact D16-Ground Handling (inc. temperature, humidity, vibration, shock) D17-Quasisteady Acceleration D18-Atomic Oxygen **<u>Environmental Models</u>** E2-Solar Particles (Solar Flare Model only; 50% confidence level) E3-Galactic Cosmic Rays (90% confidence level) E4-Trapped Radiation Belt Models (50% confidence level) **<u>Analysis</u>** A1-Thermal (System only) A2- Structural Loads (System only) A5- Particle Radiation (Total Ionizing Dose and Single Event Effects Only) A6-Electromagnetic and Magnetic Interference (Transmitters/ Receivers compatibility only) **<u>Related Management</u>** M3-Milestone Reviews (PDR, CDR, HRCR etc.) M5-Use predicted estimates only for Design Requirements (no margins) **<u>Implementation</u>** None	***As Selected (Tailored to be Project Specific)*** **Residual Risks** ***Residual Program Risk For Program Content Selected***	**<u>Testing</u>** See Testing Risk Balance Profile **<u>Environmental Design Requirements</u>** (See M5) D1-Thermal D2- Structural Loads D3-Vibration D4-Acoustic D5- Particle Radiation (Natural & on board sources, Single Event Effects) D6-Electromagnetic and Magnetic Interference D7-Electrostatic Discharge D8- Spacecraft Charging D9-Solid Particles (inc. micrometeoroids, space debris, comet dust, planetary rings) D10-Pyroshock D11-Contamination (inc. purge rqts) D12-Lightning D13-Venting and Repressurization (inc.Launch Pressure Decay, descent) D14-Surface Pressure and Atmosphere D15-Surface Impact D16-Ground Handling (inc. temperature, humidity, vibration, shock) D17-Quasisteady Acceleration D18-Atomic Oxygen **<u>Environmental Models</u>** E1-Micrometeoroids E2-Solar Particles (Flares, Plasma, Winds; 99% confidence level) E3-Galactic Cosmic Rays (90% confidence level) E4-Trapped Radiation Belts (99% confidence level) E5-Lightning (launch site) E6-Earth Space Debris E7-Planetary/Asteroid/Comet Rings, Dust E8-Planetary/Asteroid/Comet Thermal Characteristics Surface (inc. Earth) E9-Planetary Atmosphere (inc. Earth) **<u>Analysis</u>** A1-Thermal A2- Structural Loads

Very High Risk Environmental Requirements Program	Tailored Approach	Very Low Risk Environmental Requirements Program
Residual Risks 1-Lack of confidence in acceptability of H/W to meet mission needs -All analyses, A1-A20;E1,E3-E9,M5,I2 2-Unknown functional and system margins-A1,A4,A6,M5 3-Lack of robustness in tolerance to temperature excursions-A6 3-Unknown tolerance to radiation displacement damage-A4 4-Lack of verification of tolerance to Electromagnetic Compatibility, Electrostatic Discharge and spacecraft charging effects-A6, A7,A8 5-Lack of verification of tolerance to Solid Particle penetration and surface damage-A9 6-Latent H/W defects could cause a subsystem to fail or not meet its requirements-A1,A3 7-Late awareness (or lack of anticipation) of schedule, performance, and cost problems-M1,M2,M4,M5,M6,I1,I2 8-Lack of confidence in tolerance to pyroshock events-A10 9-Unknown susceptibility to particulate or volatiles or propulsion effluent contaminants-A11 10-Lack of confidence to tolerate lightning strikes at the launch pad –A12 11-Lack of confidence to tolerate venting and repressurization of cavities-A13 12-Lack of planetary protection verification-A16 13-Lack of orbital debris control verification-A17 14-Lack of confidence of surfaces to tolerate exposure to atomic oxygen-A20 15-Lack of confidence in tolerance to surface impact events-A15 16-Project progressing to the next phase of development before it is ready – M1,M3 17–Choosing the wrong/high risk contractor to develop hardware – M4,I1 18–Receiving wrong RFP responses with respect to H/W – M1,M2 19-Encountering an environment that wasn't analyzed – M1,M4,M5,M6		A3-Vibroacoustic A4- Particle Radiation (Natural & on board sources) A5-Single Event Effects A6-Electromagnetic and Magnetic Interference A7-Electrostatic Discharge A8- Spacecraft Charging A9-Solid Particle (inc. micrometeoroids, space debris, comet dust, planetary rings) A10-Pyroshock A11-Contamination (inc. purge rqts) A12-Lightning A13-Venting and Repressurization (inc.Launch Pressure Decay, descent) A14-Surface Pressure and Atmosphere A15-Surface Impact A16-Planetary Protection A17-Orbital Debris Control A18-Ground Handling (inc. temperature, humidity, vibration, shock) A19-Quasisteady Acceleration A20-Atomic Oxygen **Related Management** M1-Full Environmental Assurance Plan M2-Configuration Management M3-Milestone Reviews (PDR, CDR, HRCR etc.) M4-Project Risk Management program (See Risk Management Risk Balance Profile) M5-Use conservative margins M6-Integrated Support of Fault Protection and/or Failure Detection, Isolation & Recovery subsystems **Implementation** I1-Support Contractor Mgt. (continuous assessment w/ RFP & SEB support from env reqts) I2-Support Mission Operations and Command Assurance (MOCA) **Residual Risks** 19 - Encountering an environment that wasn't analyzed-M4, M6
Mitigations (Risk Reduction) - Maximum use of hardware with flight heritage -All (1-19) - Lessons learned-1, 19 - Strict adherence to EMC design standards-4,19 - Incentivize contractor-1,19 - Highly trained flight team familiar with hardware and software with contingency plans-1,19 - In-flight characterization-1,2,3,4,19	**Mitigations** ***Mitigations of Residual Risk Relating to Program Content Selected***	**Mitigations (Risk Reduction)** - Maximum use of hardware with flight heritage-19 - Lessons learned-19 - Strict adherence to EMC design standards-19 - Incentivize contractor-19 - Highly trained flight team familiar with hardware and software with contingency plans-19 - In-flight characterization-19 .

It is only through the thoughtful analysis of requirements upfront in the formulation phase can projects expect to achieve mission success within cost and schedule caps. The residual program risks must be understood and a "balanced" risk management approach be selected.

Summary

An approach to balance risk by making informed trades has been described. It is evermore important today's "better, faster, cheaper" projects to aggressive employ risk management decision making to achieve mission success.

Only a few examples of RBP's have been presented. Many more have been developed and will form the basis for an "Assurance Effectiveness Guidebook" developed for safety and mission assurance professionals.